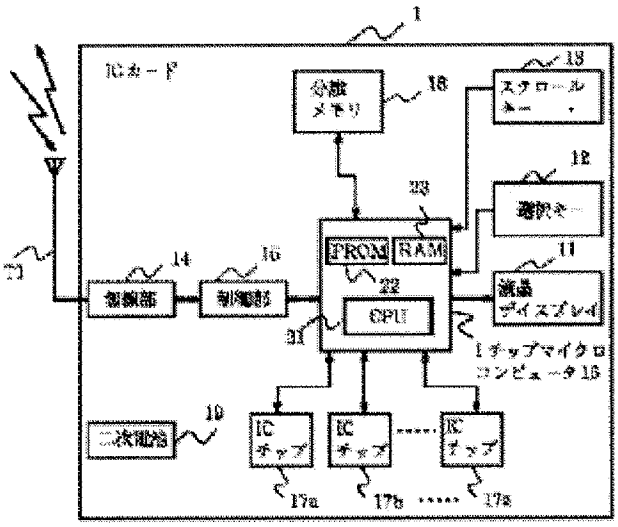
IC CARD

Publication number: JP10340231
Publication date: 1998-12-22
Inventor: OKINO EMI; SUZUKI HIROSHI
Applicant: KOKUSAI ELECTRIC CO LTD
Classification:
- international: ***G06F12/14; G06F21/24; G06K17/00; G06K19/07; G06K19/073;*** **G06F12/14; G06F21/00; G06K17/00; G06K19/07; G06K19/073;** (IPC1-7): G06F12/14; G06K17/00; G06K19/07; G06K19/073
- European:
Application number: JP19970163271 19970605
Priority number(s): JP19970163271 19970605

Abstract of **JP10340231**

PROBLEM TO BE SOLVED: To hold the security of data stored in the memory of an IC card and to collectively manage plural types of data with one IC card. SOLUTION: Plural data storage means 17a-17z store plural types of data for every type of data, and a password data storage means 22 stores password data, which have been set for every data storage means 17a-17z, for example. A collation means collates password data received from outside by input means 12 and 13 with password data and a data processing means accesses the data storage means 17a-17z where matching is obtained with the recognition of matching as a condition. A separation memory 18 stores data of comparatively high secrecy and access from the data processing means to the separation memory 18 is made possible only when an access request from an external reader/ writer where access right to the separation memory 18 is set is given.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－340231

(43)公開日　平成10年(1998)12月22日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	12/14	３２０	Ｃ０６Ｆ	12/14	３２０Ｃ
Ｇ０６Ｋ	17/00		Ｃ０６Ｋ	17/00	Ｅ
					Ｔ
	19/073			19/00	Ｐ
	19/07				Ｎ

審査請求　未請求　請求項の数２　ＦＤ　(全 19 頁)

(21)出願番号　特願平9－163271

(22)出願日　平成９年(1997)６月５日

(71)出願人　000001122
国際電気株式会社
東京都中野区東中野三丁目14番20号

(72)発明者　沖野　恵美
東京都中野区東中野三丁目14番20号　国際電気株式会社内

(72)発明者　鈴木　浩
東京都中野区東中野三丁目14番20号　国際電気株式会社内

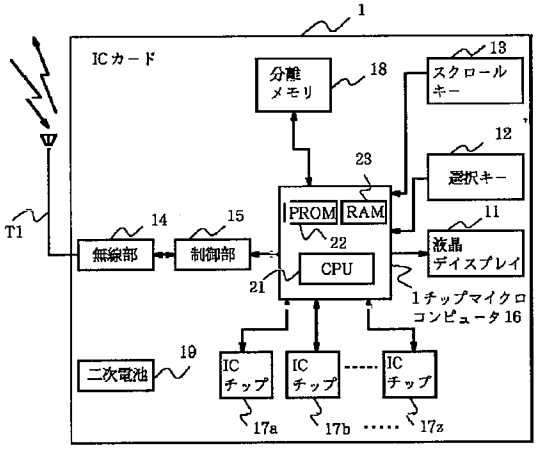
(74)代理人　弁理士　守山　辰雄

(54)【発明の名称】　ＩＣカード

(57)【要約】

【課題】　ＩＣカードのメモリに記憶されるデータの安全性（セキュリティ）を担保する。また、１枚のＩＣカードで複数種類のデータを一括管理する。

【解決手段】　例えば複数のデータ記憶手段１７ａ～１７ｚにより複数種類のデータをデータの種類毎に記憶し、パスワードデータ記憶手段２２により各データ記憶手段１７ａ～１７ｚ毎に設定されたパスワードデータを記憶する。そして、照合手段１６が例えば入力手段１２、１３により外部から受け付けたパスワードデータを上記パスワードデータと照合し、これらの一致が確認されたことを条件に、データ処理手段１６が当該一致が得られたデータ記憶手段１７ａ～１７ｚへアクセスする。また、例えば分離メモリ１８により比較的秘匿性が高いデータを記憶し、当該分離メモリ１８へのアクセス権が設定された外部のリーダ・ライタからのアクセス要求があった場合にのみ、データ処理手段１６から分離メモリ１８へのアクセスを可能とする。



【特許請求の範囲】
【請求項１】　データを記憶して処理するＩＣカードにおいて、
複数種類のデータをデータの種類毎に記憶する複数のデータ記憶手段と、
各データ記憶手段毎に設定されたパスワードデータを記憶するパスワードデータ記憶手段と、
外部から入力されたパスワードデータを受け付ける入力手段と、
入力されたパスワードデータとパスワードデータ記憶手段に記憶されているパスワードデータとを照合する照合手段と、
照合手段によりパスワードデータの一致が確認されたことを条件に、当該一致が得られたデータ記憶手段へアクセスするデータ処理手段と、
を備えたことを特徴とするＩＣカード。
【請求項２】　外部のリーダ・ライタとの間でデータの通信を行うＩＣカードにおいて、
データを記憶するデータ記憶手段と、
データ記憶手段へアクセスするデータ処理手段と、
データ記憶手段に記憶されるデータに比べて秘匿性が高いデータを記憶する分離メモリと、
分離メモリへのアクセス権が設定されたリーダ・ライタを管理する管理手段と、
リーダ・ライタからのアクセス要求に対して、当該リーダ・ライタが管理手段により分離メモリへのアクセス権を有しているものとして管理されているか否かの認証を行う認証手段と、
分離メモリがデータ処理手段によりアクセスされることを禁止する一方、認証手段によりアクセス権が認められたことを条件に、リーダ・ライタからの要求に応じてデータ処理手段に分離メモリへアクセスさせる分離メモリアクセス制御手段と、
を備えたことを特徴とするＩＣカード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データを記憶して処理するＩＣカードに関し、特に、複数種類のデータをデータの種類毎に安全性（セキュリティ）を担保して一括管理するＩＣカード及びメモリ（分離メモリ）へのアクセスを制御することにより当該メモリ（分離メモリ）に記憶されている秘匿性が高いデータの安全性を担保するＩＣカードに関する。
【０００２】
【従来の技術】ＩＣカードは、一般に、ＩＣメモリやＣＰＵ等が埋め込まれたカードのことであり、例えばクレジットカードやキャッシュカードとして用いられている。また、ＩＣカードは、例えば磁気カードに比べて記憶容量を大幅に増大させることができるといった利点や、ＩＣカードの内部でデータの演算処理等を行うことができるといった利点から磁気カード等といった磁気記録媒体に代わるものとして注目されている。このため、例えばキャッシュカード会社が発行する上記したキャッシュカードや、小口決済等に用いられる電子マネーと呼ばれる電子財布等、種々の分野において、上記したような磁気カードからＩＣカードへの移行の試みがなされている。
【０００３】また、ＩＣカードが適用される分野としては、上記したキャッシュカードやクレジットカード等といった金融関連の分野に限られず、例えば学生証や社員証や健康保険証や運転免許証といった各種の身分証明書や定期券等といったものについても、ＩＣカードは、広く応用され得るものである。このようなＩＣカードを利用する利用者は、例えばキャッシュカードとしての機能を有するＩＣカードや、自己の身分証明書のデータが記憶されたＩＣカード等といった各データの種類毎に発行されたＩＣカードを携帯し、必要に応じてこれらのカードにより決済や身分証明等を行う。
【０００４】
【発明が解決しようとする課題】しかしながら、上記のようなＩＣカードでは、１枚のＩＣカードには１種類のデータしか記憶されておらず、このため、利用者が例えばクレジットや電子マネーや身分証明といった複数種類のデータをＩＣカードで管理したい場合には、これら複数種類のデータに応じて、複数枚のＩＣカードを携帯しなければならないといった不具合があった。すなわち、例えば、利用者はクレジットカードとして用いられるＩＣカードや身分証明として用いられるＩＣカード等といった複数枚のＩＣカードを日常生活において財布等に入れて持ち運ばなくてはならず、このため、利用者にとって荷物がかさばってしまうといった不具合や、また、ＩＣカードの使用に際して、複数枚のＩＣカードを各カードの機能毎に使い分けなければならないといった不便さがあった。
【０００５】また、例えば、企業独自にクレジットや身分証明等といった複数種類のデータを一括管理するコーポレートカードを導入することにより、カードの利用性を向上させるとともに事務処理の合理化に役立てたいといった要求があった。また、情報化社会の進展や消費者の生活様式の変化等に伴い、ＩＣカードによるデータの保管や処理等にかかるコストを減少させるために、１枚のＩＣカードに複数種類のデータを記憶させて処理させたいといった要求があった。このように、従来では、各データの種類毎に発行されるＩＣカードが用いられており、利用者にとっての利便性が良くない等といった不具合があったため、複数種類のデータを一括管理するＩＣカードの実現が望まれていた。
【０００６】また、ＩＣカードに記憶されるクレジットや身分証明等といったデータの中には、一般に、第三者等に漏洩してしまうことを防止する必要がある秘匿性が

高いデータが含まれており、このような秘匿性が高いデータの安全性（セキュリティ）を確保しなければならないといった要求があった。また、同様に、例えば利用者がＩＣカードを紛失してしまった場合であっても、当該ＩＣカードが第三者により不正に使用されてしまうことや、ＩＣカードに記憶されているデータが不正に偽造或いは改ざん等されてしまうことを防止しなければならないといった要求があった。このようにＩＣカードでは、例えば記録されているデータの読み取りが比較的容易な上記従来例で示した磁気カードに比べれば安全性が比較的確保されてはいるものの、まだ十分ではなく、更にデータの安全性を高めたいといった要求があった。

【０００７】本発明は、このような従来の課題を解決するためになされたもので、複数種類のデータを記憶及び処理等することができるＩＣカードを提供することを目的とする。また、本発明は、メモリに記憶されるデータの第三者への漏洩等を防止して、当該データの安全性（セキュリティ）を担保することができるＩＣカードを提供することを目的とする。更に具体的には、複数種類のデータを１枚のＩＣカードで記憶して処理等することができ、且つ、これら複数種類のデータをデータの種類毎に安全性を担保して保持することができるＩＣカードを提供することを目的とする。また、外部のリーダ・ライタとの間でデータの通信を行うＩＣカードにおいて、メモリ（分離メモリ）に記憶される秘匿性が高いデータの安全性を担保することができるＩＣカードを提供することを目的とする。

【０００８】

【課題を解決するための手段】上記目的を達成するため、本発明に係るＩＣカードでは、複数種類のデータをデータの種類毎に記憶する例えばメモリから構成される複数のデータ記憶手段を備え、次のようにして各データ記憶手段へのアクセスを制御する。すなわち、ＩＣカードでは、パスワードデータ記憶手段により各データ記憶手段毎に設定されたパスワードデータが記憶されており、入力手段が外部から入力されたパスワードデータを受け付けた場合には、照合手段が入力されたパスワードデータとパスワードデータ記憶手段に記憶されているパスワードデータとを照合する。そして、この照合の結果、パスワードデータの一致が確認されたことを条件に、データ処理手段が当該一致が得られたデータ記憶手段へアクセスする。

【０００９】従って、複数種類のデータがデータの種類毎に記憶され、且つ、これら各データの種類毎にパスワードデータが設定されているため、各データの種類毎に正しいパスワードデータが入力されないと、例えばＣＰＵ等から構成されるデータ処理手段により当該種類のデータ記憶手段へアクセスすることができない。このため、各種類毎のデータの安全性（セキュリティ）を担保しつつ、これら複数種類のデータを１枚のＩＣカードで一括管理することができる。ここで、本発明で言うアクセスとは、データ記憶手段に記憶されているデータを読み出すことや、書き換えることや、削除することや、また、データ記憶手段に新規なデータを記憶させること等を言う。

【００１０】また、本発明に係るＩＣカードでは、データを記憶するデータ記憶手段と、データ記憶手段へアクセスするデータ処理手段と、データ記憶手段に記憶されるデータに比べて秘匿性が高いデータを記憶する分離メモリとを備え、外部のリーダ・ライタとの間でデータの通信を行うに際して、次のようにして分離メモリへのアクセスを制御する。すなわち、ＩＣカードでは、管理手段が分離メモリへのアクセス権が設定されたリーダ・ライタを管理し、認証手段がリーダ・ライタからのアクセス要求に対して、当該リーダ・ライタが管理手段により分離メモリへのアクセス権を有しているものとして管理されているか否かの認証を行う。そして、分離メモリアクセス制御手段が認証手段によりアクセス権が認められたことを条件に、リーダ・ライタからの要求に応じてデータ処理手段に分離メモリへアクセスさせる。また、認証手段によりアクセス権が認められた場合を除いては、分離メモリアクセス制御手段は、分離メモリがデータ処理手段によりアクセスされることを禁止する。

【００１１】従って、分離メモリへのアクセス権が設定された外部のリーダ・ライタからのアクセス要求があった場合にのみ、例えばＣＰＵ等から構成されるデータ処理手段により分離メモリへアクセスすることができる一方、この場合を除いてはデータ処理手段は分離メモリへアクセスすることができないため、分離メモリに記憶される秘匿性が高いデータの第三者への漏洩等を防止して、当該データの安全性（セキュリティ）を担保することができる。ここで、本発明で言うアクセスとは、上記と同様に、分離メモリやデータ記憶手段に記憶されているデータを読み出すことや、書き換えることや、削除することや、また、分離メモリやデータ記憶手段に新規なデータを記憶させること等を言う。

【００１２】また、例えば上記した分離メモリに、リーダ・ライタへアクセスするためのＩＤを記憶させておくことにより、ＩＣカードとリーダ・ライタとの間で相互認証を行うようにするのが好ましく、このようにＩＣカード側とリーダ・ライタ側とで互いに相手側を認証するようにすることにより、不正なＩＣカードや不正なリーダ・ライタとの間でデータの通信が行われてしまうのを防止することができる。

【００１３】

【発明の実施の形態】本発明に係る一実施例を図面を参照して説明する。図１には、本発明に係るＩＣカードを用いたＩＣカードシステムの一例を示してあり、このシステムには、本発明に係るＩＣカード１と、ＩＣカード１との間でデータの通信を行うリーダ・ライタである仲

介器２と、仲介器２との間でデータの通信を行うシステム管理装置３とが備えられている。また、システム管理装置３には回線４ａを介してＡＴＭ（Asynchronous Transfer Mode）交換機５が接続されており、このＡＴＭ交換機５には、通信販売会社６に備えられたＬＡＮ７及び官公庁機関８に備えられたコンピュータ９がそれぞれ回線４ｂ及び回線４ｃを介して接続されている。また、本例では、例えば加入者回線から成る上記した回線４ａ、４ｂ、４ｃとＡＴＭ交換機５とからデジタル伝送を行うための広帯域統合サービスデジタル網（Ｂ－ＩＳＤＮ：Broadband-Integrated Services Digital Network）が構成されている。

【００１４】なお、上記したＢ－ＩＳＤＮは、上記したＡＴＭ交換機５や光ファイバ伝送を中核としてテレビ信号や超高速データの伝送を可能とするＩＳＤＮであり、例えば電話による音声データや、テキストデータや、ファクシミリによる通信データや、画像データといった種々の通信サービスを１つのデジタルネットワークで提供することができるものである。また、上記したＡＴＭ交換機５は、例えば音声データや画像データといった回線交換向きのデータや、例えばテキストデータといったパケット交換向きのデータを同一の装置で中継することができ、また、ビットレートが異なった種々のデータが混在している場合であっても正しく動作するため、例えば需要動向が確定されないＢ－ＩＳＤＮに最適のものである。

【００１５】ここで、図１では、１枚のＩＣカード１のみを示してあるが、ＩＣカード１を利用する利用者が複数存在する場合には、これら各利用者に対してＩＣカード１が発行されるため、複数枚のＩＣカード１が存在し、発行されたこれらのＩＣカード１は各利用者によって所持される。また、仲介器２は、例えば上記した通信販売会社６や官公庁機関８や、また、銀行やクレジットカード会社等により設置され、各利用者が所持するＩＣカード１との間でデータの通信を行う。なお、図１では、１つの仲介器２のみを示してあるが、この仲介器２としても、例えば各会社や機関毎に、また、例えば一定の地域毎にといったように、本例では複数の仲介器２が設置されているとする。

【００１６】また、本例では、これらＩＣカード１や仲介器２はＩＣカードシステムを管理するシステム供給者により供給及び管理されており、システム供給者は上記したシステム管理装置３により、複数の会社や機関等によって設置された複数の仲介器２や複数の利用者によって所持されているＩＣカード１をまとめて管理する。ここで、利用者に提供される各ＩＣカード１や、会社や機関等によって設置される各仲介器２には、各ＩＣカード１及び各仲介器２を識別するための固有のＩＤがシステム供給者により割り当てられて格納されており、本例ではこのＩＤによりＩＣカード１と仲介器２との間で相互に認証を行う。

【００１７】また、本例では、公開鍵デジタル署名方式として知られる暗号方式によりＩＣカード１と仲介器２との間でデータの通信を行うこととし、このため、各ＩＣカード１と各仲介器２には、システム供給者により割り当てられた固有の署名関数及び検査関数が格納される。ここで、署名関数は通信対象となるデータを暗号化するための関数であり、また、検査関数は、署名関数により暗号化されたデータを元のデータに復号化する関数であって、署名関数とは異なった関数が用いられている。更に具体的には、署名関数を秘密にしておき、この署名関数により暗号化されたデータと検査関数のみとを送信相手へ送信することにより、これらのデータを受信した当該送信相手がこれらのデータから署名関数を再生することを至難化して、データの偽造等を防止している。

【００１８】なお、暗号方式としては他の種類の暗号方式が用いられてもよく、また、本発明では必ずしも上記のような暗号方式が用いられなくてもよく、これらはシステムの利用状況等に応じて任意に設定されてよい。また、本例では、データの安全性（セキュリティ）を更に高めるため、上記したＩＤや検査関数には、システム供給者によりこれらが正当なものであることを証明するデジタル署名が施され、また、各ＩＣカード１や仲介器２には、システム供給者のデジタル署名を検査するための供給者検査関数が上記した署名関数と共に格納される。これにより、ＩＣカード１や仲介器２では、ＩＣカードシステムに共通な供給者検査関数を有していない相手との間で不正な或いは誤った通信及び取引をしてしまうことを防止することができる。

【００１９】また、本例では、ＩＣカード１として無線データの通信を行う非接触型ＩＣカードを用いることとし、これによりＩＣカード１は、アンテナＴ２を備えた仲介器２との間で無線データの通信を行う。なお、本例では、非接触型ＩＣカード１として、仲介器２の近くに寄る程度で当該仲介器２との間で無線データの通信が可能になる近接型の非接触型ＩＣカードを用いる。また、同様に、本例では、仲介器２とシステム管理装置３との間においても、システム管理装置３に備えられたアンテナＴ３を介して無線データの通信を行う。

【００２０】なお、ＩＣカード１としては、必ずしも非接触型のＩＣカードが用いられる必要はなく、例えば仲介器２と直接的に接点で接続されてデータの通信を行う接触型のＩＣカードが用いられてもよく、また、例えば無線による非接触型の通信と接点による接触型の通信との両方を行うことができるＩＣカードが用いられてもよい。また、仲介器２とシステム管理装置３との間のデータ通信についても同様に、有線による通信が行われてもよい。以上に示した構成により、上記したＩＣカードシステムでは、ＩＣカード１と仲介器２との間でデータの

通信を行うことにより決済取引等といった処理を行い、また、これらＩＣカード１や仲介器２によって行われる取引処理の状況等をシステム管理装置３により一括管理する。また、システム管理装置３では、Ｂ－ＩＳＤＮを介して通信販売会社６に備えられたＬＡＮ７や官公庁機関８に備えられたコンピュータ９等といった各会社や機関に備えられたコンピュータ等との間でデータの通信を行うこともできる。

【００２１】次に、本発明に係るＩＣカード１の外観の一例を図２に示す。同図に示したＩＣカード１には、データを表示する液晶ディスプレイ１１と、電源のオン、オフ等を行うための選択キー１２と、データを入力等するためのスクロールキー１３とが備えられている。液晶ディスプレイ１１は、ＩＣカード１に記憶されているデータや仲介器２から受信したデータ等を表示する表示器である。なお、この表示器としては、必ずしも液晶ディスプレイが用いられる必要はなく、データを表示することができれば任意の表示器が用いられてもよい。

【００２２】選択キー１２は、ＩＣカード１の利用者（携帯者）により操作され、ＩＣカード１の電源をオフにする”ＯＦＦ”と、ＩＣカード１の電源をオンにする”ＯＮ”と、モードの切替を行うための”モード”とのいずれかを選択するためのキーである。ここで、本例では、モードの切替として、例えば現在の日時を表示するモードや、仲介器２との間でデータの通信を行うモードといった各種のモードの切り替えが行われる。

【００２３】スクロールキー１３は、ＩＣカード１の利用者により操作され、データの入力やＩＣカード１に対しての各種指示等を行うためのキーである。例えば、選択キー１２で”モード”を選択することによって切替可能なモードを表示させ、このスクロールキー１３で切り替えたいモードを選択することにより、モードの切替処理が行われる。また、例えばＩＣカード１にデータを入力するモードでは、液晶ディスプレイ１１上にアルファベットや数字等が表示され、スクロールキー１３で入力したい文字を選択することにより、データの入力処理が行われる。なお、選択キー１２やスクロールキー１３の構成としては、本例に示したものに限られず、例えばキーボードのように各アルファベットや数字等に対応した複数のキーを備えたものであってもよい。

【００２４】次に、図３には、上記した本発明に係るＩＣカード１の一構成例を示してあり、このＩＣカード１には、上記した液晶ディスプレイ１１、選択キー１２、スクロールキー１３と、アンテナＴ１と、無線データの通信を行う無線部１４と、当該通信の制御を行う制御部１５と、データの処理を行う１チップマイクロコンピュータ１６と、データを記憶する複数のＩＣチップ１７ａ、１７ｂ、・・・、１７ｚと、これら各処理部１１～１６、１７ａ～１７ｚ及び後述する分離メモリ１８に電源を供給する二次電池１９とが備えられている。なお、上記したように、分離メモリ１８については後述する。

【００２５】アンテナＴ１は、仲介器２から送信された無線データを受信する例えばループアンテナから構成されている。ここで、ループアンテナは、一般に、携帯無線機器等に広く利用されているアンテナであり、このループアンテナの構成例を図４に示す。なお、ループアンテナは一般に利用されているものであるため、以下の説明においてその詳細については省略する。図４（ａ）には、銅体に銀メッキを施したアンテナであるＲＦループアンテナ３１の一例を示してあり、このアンテナ３１は、透明オーバーシート３２ａ及び３２ｂによって囲まれた白色コア３３や整合回路３４等から構成されている。図４（ｂ）には、渦巻状薄膜アンテナ３５の一例を示してあり、このアンテナ３５は、渦巻状の薄膜３６や整合回路３７等から構成されている

【００２６】図４（ｃ）には、導体板を利用したループアンテナ３８の一例を示してあり、このアンテナ３８・は、導体板４０ａ及び４０ｂやこれらを短絡する短絡導体３９や給電点４１や整合回路４２等から構成されている。ここで、上記したように、各アンテナ３１、３５、３８には、給電率の整合をとるための整合回路３４、３７、４２がそれぞれ備えられており、これらの整合回路３４、３７、４２から各アンテナ３１、３５、３８における給電が行われる。また、図４（ｄ）には、これら整合回路３４、３７、４２の等価回路４３の一例を示してある。

【００２７】同図（ｄ）に示した等価回路４３では、アンテナ側と給電系側とが導体によりコイルＬを介して接続されており、また、コイルＬの両端はそれぞれコンデンサＣ１或いはＣ２を介して接地されている。ここで、コンデンサＣ１及びＣ２としては、例えば集中定数のコンデンサや、導体の端子とアンテナのケースとの間のストレーキャパシティによるコンデンサ等が用いられ、また、コイルＬとしては、例えば導線を渦巻状に巻いたコイルや、白色コア３３内にパターン形成されたコイル等が用いられる。なお、アンテナＴ１としては、上記したものに限られず、仲介器２との間で無線データを通信することができるものであれば、どのようなアンテナが用いられてもよい。

【００２８】無線部１４は、例えば無線データの変調処理を行う変調器や復調処理を行う復調器から構成されており、アンテナＴ１を介して仲介器２との間で無線データの通信を行う。すなわち、無線部１４は、例えば仲介器２から受信した無線信号を復調するとともに当該信号の強度を増幅させ、当該信号の波形を制御部１５により読み取ることができるような波形に変換して制御部１５へ出力する。制御部１５は、例えばＣＰＵやメモリ等から構成されており、無線部１４により仲介器２から受信されたデータが自己宛のデータであるか否かを判定する。すなわち、本例では、後述する１チップマイクロコ

ンピュータ１６に備えられたＰＲＯＭ（プログラマブルＲＯＭ）には、各ＩＣカード１毎に予め設定された呼出番号が格納されており、制御部１５は、この自己に設定されている呼出番号を読み出し、読み出した番号と受信された無線データの先頭等に含まれている宛先番号（選択信号）とが一致するか否かを判定することにより、当該データが自己宛のデータであるか否かを判定する。

【００２９】そして、この判定の結果、両者の番号が一致して当該データが自己宛のデータであると判定された場合には、制御部１５は、この無線データを送信した仲介器２との間でデータの通信を行うために、受信された例えば選択信号に引き続く情報信号といったデータを１チップマイクロコンピュータ１６へ出力させる。１チップマイクロコンピュータ１６には、各種演算や判断等の処理を行うＣＰＵ（中央処理装置）２１と、上記した呼出番号等を格納するＰＲＯＭ２２と、ＣＰＵ２１が行う各種演算等の処理領域となるＲＡＭ（ランダムアクセスメモリ）２３とが内蔵されており、ＣＰＵ２１がＰＲＯＭ２２に格納された制御プログラムをＲＡＭ２３に展開して実行することにより、ＩＣカード１における各種処理や管理処理等を実行し、ＩＣカード１全体を統括制御する。

【００３０】ここで、ＰＲＯＭ２２には、上記した呼出番号と共に、上記した暗号方式に従ってデータの通信処理を行うための制御プログラムや、日時の計数処理を行うための制御プログラム等といった各種の処理を行うための制御プログラムが格納されている。また、ＰＲＯＭ２２には、後述する各ＩＣチップ１７ａ～１７ｚ毎に設定されたパスワードデータが記憶されており、本例では、メモリ等から構成されているこのＰＲＯＭ２２がパスワードデータを記憶するパスワードデータ記憶手段である。

【００３１】また、ＰＲＯＭ２２には、ＩＣカード１の外部から入力されたパスワードデータと、自己に記憶されている上記したパスワードデータとが一致するか否かを照合する制御プログラムが格納されており、本例では、ＣＰＵ２１がＰＲＯＭ２２に格納された当該制御プログラムをＲＡＭ２３に展開して実行することにより、上記の照合処理を行う照合手段が構成される。ここで、ＩＣカード１へのパスワードデータの入力としては、例えば利用者が上記した操作キー１２やスクロールキー１３を操作することにより入力され、また、例えば仲介器２から無線送信されてきたパスワードデータをアンテナＴ１を介して無線部１４が受信することにより入力される。すなわち、本例では、選択キー１２やスクロールキー１３により、また、アンテナＴ１及び無線部１４により、外部から入力されたパスワードデータを受け付ける入力手段が構成される。

【００３２】また、本例では、上記した照合手段によりパスワードデータの一致が確認されたことを条件に、ＣＰＵ２１がＰＲＯＭ２２に格納された所定の制御プログラムをＲＡＭ２３に展開して実行し、当該一致が得られたＩＣチップ（ＩＣチップ１７ａ～１７ｚのいずれか）へアクセスすることによりデータ処理手段が構成される。なお、上記したように、本例で言うアクセスとは、ＩＣチップ１７ａ～１７ｚや後述する分離メモリ１８に記憶されているデータを読み出すことや、書き換えることや、削除することや、また、ＩＣチップ１７ａ～１７ｚや分離メモリ１８に新規なデータを記憶させること等を示す。

【００３３】また、ＲＡＭ２３では、例えば仲介器２から受信されたメッセージデータ（メッセージ信号）を記憶することも行われ、このメッセージ信号は、例えば無線部１４及び制御部１５を介して１チップマイクロコンピュータ１６へ入力された際に、ＣＰＵ２１等により解読される。また、このようにして解読されたメッセージ信号の内容は、上記した選択キー１２やスクロールキー１３により、液晶ディスプレイ１１に表示させることもできる。ＩＣチップ１７ａ～１７ｚは、データを記憶するメモリから構成されるデータ記憶手段であり、本例では、複数種類のデータをデータの種類毎に記憶する。ここで、本例では、複数種類のデータをデータの種類毎に記憶するために複数のＩＣチップ１７ａ～１７ｚが備えられているが、必ずしもこのような構成でなくてもよく、例えば１つのメモリの記憶領域がデータの種類毎に複数の領域に分割されて用いられてもよい。また、本例では、ＩＣチップ１７ａ～１７ｚの２６個のＩＣチップをＩＣカード１に備えたが、ＩＣチップとしては、ＩＣカード１に記憶させるデータの種類の数等に応じて任意の数のＩＣチップが備えられてよい。

【００３４】上記したＩＣチップ１７ａ～１７ｚには、例えばＩＣチップ１７ａにはクレジットのデータが記憶され、また、例えばＩＣチップ１７ｂには身分証明のデータが記憶され、また、例えばＩＣチップ１７ｃには利用者によって入力されたメモデータが記憶されるといったように、複数種類のデータがデータの種類毎に記憶される。また、上記したように、各ＩＣチップ１７ａ～１７ｚにはそれぞれ、パスワードデータが設定され、このようにデータの種類毎に設定されたパスワードデータを利用者や仲介器２がＩＣカード１に正しく入力しなければ、上記したＣＰＵ２１等から構成されるデータ処理手段により当該種類のデータを記憶するＩＣチップ１７ａ～１７ｚへアクセスすることができない。

【００３５】これにより、ＩＣカード１では、クレジットカードとしてのデータやキャッシュカードとしてのデータや身分証明書としてのデータ等といった複数種類のデータを１枚のカードで一括管理することができ、且つ、例えばこれら各データの種類毎に異なったパスワードデータを設定することにより、これらのデータが第三者により改ざん等されてしまうことを防止して、データ

の種類毎に複数種類のデータの安全性を担保することができる。なお、本例では、上記したパスワードデータは利用者により設定されるものとし、また、後述する図１０で示すように、これらのパスワードデータは利用者により変更が可能であるとする。ここで、パスワードデータとしては、例えば、仲介器２を設置するクレジットカード会社等によって設定されてもよい。

【００３６】また、例えば、ＩＣカード１の利用者によって用いられるパスワードデータと仲介器２によって用いられるパスワードデータとを異ならせてもよく、このようにした場合には、利用者は自己にしか知得されないパスワードデータを各種類のデータ毎に設定することができ、これにより、データの安全性を更に高めることができる。なお、この場合には、上記した１チップマイクロコンピュータ１６に備えられたＰＲＯＭ２２には、利用者により用いられるパスワードデータと仲介器２により用いられるパスワードデータとを共に格納しておく。そして、パスワードデータの照合に際しては、ＣＰＵ２１等により、当該パスワードデータが利用者によって選択キー１２やスクロールキー１２により入力されたものであるのか、或いは、仲介器２からアンテナＴ１を介して無線部１４により受信入力されたものであるのかを判定し、この判定結果に従って、利用者に設定されたパスワードデータと仲介器２に設定されたパスワードデータとを使い分けて照合処理を行う。

【００３７】二次電池１９は、ＩＣカード１に備えられた各処理部１１～１６、１７ａ～１７ｚ及び後述する分離メモリ１８に駆動電力を供給する電池であり、本例では、例えばリチウムイオン電池といった二次電池が用いられている。ここで、この二次電池１９は、例えば電磁誘導方式を用いて充電され、この方式による充電処理の一例を図５を用いて説明する。同図には、ＩＣカード１と、当該ＩＣカード１の二次電池１９を充電させる充電器５１とが示されている。ここで、充電器５１には、例えばトランスから構成される電源アダプタ５２と、直流電流と交流電流とを変換するインバーター回路５３と、例えば渦巻状の導通線から構成されるコイル５４とが備えられている。

【００３８】また、図５に示したＩＣカード１には、例えば渦巻状の導通線から構成されるコイル５５と、交流電流を直流電流に変換する整流器５６と、上記した二次電池１９とが備えられている。なお、コイル５５と整流器５６については、上記図３では図示を省略してある。これらの装置により充電処理を行うに際しては、まず、充電器５１では、例えば受電されたＡＣ１００Ｖ（１００ボルトの交流電圧）を電源アダプタ５２により直流電流に変換し、変換された直流電流をインバーター回路５３に通電して交流電流に変換する。そして、この変換された交流電流がコイル５４に流れて交流磁界が発生する。

【００３９】一方、図５に示すように、充電処理に際しては、ＩＣカード１のコイル５５が充電器のコイル５４に近接するように設置され、ＩＣカード１では、まず、上記のように充電器５１のコイル５４で発生した交流電流エネルギーがＩＣカード１のコイル５５により受け取られる。そして、この受け取られた交流磁界エネルギーに起因してコイル５５に発生した交流電流が整流器５６により直流電流に変換され、この変換された直流電流により二次電池１９が充電される。なお、ＩＣカード１の電力供給方法としては、必ずしも本例のように二次電池が用いられなくてもよく、ＩＣカード１に電力を供給することができるものであれば、例えば一次電池といった任意の電力供給手段が用いられてもよい。

【００４０】以上のように、上記したＩＣカード１では、各データの種類毎にパスワードデータを設定することによりこれら各種類毎のデータの安全性を担保しつつ、複数種類のデータを１枚のＩＣカードにより一括管理することができる。すなわち、例えば、各ＩＣチップ１７ａ～１７ｚ毎に異なったパスワードデータを設定することにより、或る種類のデータを記憶するＩＣチップ１７ｔに設定されたパスワードデータが第三者に漏洩等してしまった場合であっても、他の種類のデータについては不正な改ざん等が行われてしまうことを防止することができ、このように、複数種類のデータを一括管理しつつ、これらのデータの安全性をデータの種類毎に担保することができる。

【００４１】ここで、上記図３に示した分離メモリ１８について説明する。分離メモリ１８は、データを記憶するメモリから構成されており、本例のようにＩＣカード１に分離メモリ１８が備えられた場合には、例えば上記したＩＣチップ１７ａ～１７ｚに記憶されるデータに比べて秘匿性が高いデータがこの分離メモリ１８に記憶される。ここで、本例で言う秘匿性が高いデータとは、例えば第三者に知られてしまうことを防止する必要がある暗証番号等といったデータや、また、例えば不正に改ざんされてしまうことを防止する必要がある免許証番号等といったデータのことを言い、すなわち、第三者等により不正に利用等されてしまうことを防止する必要があるデータのことを言う。

【００４２】また、本例では、この分離メモリ１８には、秘匿性が高いデータとして、取引プロトコルに必要なデータである上記したＩＣカード１のＩＤといったデータや、上記した所定の暗号方式に必要な署名関数や検査関数といったデータや、各種クレジットカードや証明書等の暗証番号（パスワード）といったデータや、各種身分証明のデータの中で秘匿性が高いデータや、また、例えば決済に関しての過去の取引内容や資金価値等を示す残高データといったデータ等が記憶される。

【００４３】上記した分離メモリ１８へは、当該分離メモリ１８へのアクセス権が設定された仲介器（リーダ・

ライタ）２からのアクセス要求がなければ、１チップマイクロコンピュータ１６によりアクセスすることができず、この分離メモリ１８へのアクセス制御について更に詳しく説明する。このアクセス制御において、ＩＣチップ１７ａ～１７ｚは、上記と同様に、データを記憶するデータ記憶手段であり、ＩＣカード１に分離メモリ１８が備えられた場合には、これらＩＣチップ１７ａ～１７ｚには、分離メモリ１８に記憶されるデータに比べて秘匿性が低いデータや、ＩＣカード１の利用者によりいつでも確認することができることが要求されるデータ等が記憶される。

【００４４】すなわち、この場合に、ＩＣチップ１７ａ～１７ｚには、例えばこれら各ＩＣチップ１７ａ～１７ｚに記憶されているデータの種類（名称）を示すデータや、クレジットについての未決済額のデータや、預金についての現在の所持残高の金額を示す記録データ等が記憶される。これにより、利用者は、上記したパスワードデータを用いて記録データ等のデータを液晶ディスプレイ１１に表示させることができ、預金の残高等を確認することができる。なお、分離メモリ１８には、秘匿性が高いデータと共に、上記したような比較的秘匿性が低いデータをも記憶させておくこともでき、本例では、分離メモリ１８に上記した記録データを記憶させておく。

【００４５】また、１チップマイクロコンピュータ１６のＰＲＯＭ２２には、分離メモリ１８へのアクセス権が設定された仲介器２に割り当てられているＩＤが格納されており、本例では、このＰＲＯＭ２２が、分離メモリ１８へのアクセス権が設定された仲介器２（リーダ・ライタ）を管理する管理手段である。また、ＰＲＯＭ２２には、仲介器２（リーダ・ライタ）からのアクセス要求に対して、当該仲介器２が上記した管理手段により分離メモリ１８へのアクセス権を有しているものとして管理されているか否かの認証を行う制御プログラムが格納されている。

【００４６】すなわち、本例では、この認証処理を上記したＩＤによって行い、仲介器２から通知されたＩＤがＰＲＯＭ２２に格納されている場合には、当該仲介器２にアクセス権が設定されていると判定し、これとは逆に、通知されたＩＤがＰＲＯＭ２２に格納されていない場合には、アクセス権が設定されていないと判定する。また、本例では、１チップマイクロコンピュータ１６のＣＰＵ２１がＰＲＯＭ２２に格納された上記の制御プログラムをＲＡＭ２３に展開して実行することにより上記認証処理を行う認証手段が構成される。

【００４７】また、本例では、上記と同様に、ＣＰＵ２１がＰＲＯＭ２２に格納された所定の制御プログラムをＲＡＭ２３に展開して実行することにより、データ記憶手段であるＩＣチップ１７ａ～１７ｚへアクセスするデータ処理手段が構成される。ここで、このデータ処理手段は、上記した認証手段により、分離メモリ１８へのアクセス権が設定された仲介器２からアクセス要求があったと認証された場合にのみ分離メモリ１８へアクセスすることができ、この条件が満たされない場合には、分離メモリ１８へアクセスすることが禁止されている。

【００４８】本例では、この分離メモリ１８へのアクセス制御を行う制御プログラムがＰＲＯＭ２２に格納されており、ＣＰＵ２１がＰＲＯＭ２２に格納された当該制御プログラムをＲＡＭ２３に展開して実行することにより、分離メモリ１８が上記したＣＰＵ２１等から構成されるデータ処理手段によりアクセスされることを禁止する一方、上記した認証手段によりアクセス権が認められたことを条件に、仲介器（リーダ・ライタ）２からの要求に応じてデータ処理手段に分離メモリ１８へアクセスさせる分離メモリアクセス制御手段が構成される。

【００４９】ここで、本実施形態では、例えばプロセッサやメモリ等を備えたハードウェア資源において、ＣＰＵ２１がＰＲＯＭ２２に格納された所定の制御プログラムを実行することにより、分離メモリ１８へのアクセス制御処理及び上記したデータの種類毎に設定されたパスワードデータによる複数種類のデータの一括管理処理を制御する構成としたが、本発明では、これらの処理を実行するための各機能手段を独立したハードウェア回路として構成してもよい。また、本発明は上記の制御プログラムを格納したフロッピーディスクやＣＤ－ＲＯＭ等のコンピュータにより読み取り可能な記憶媒体として把握することもでき、当該制御プログラムを記憶媒体からコンピュータに入力してプロセッサに実行させることにより、本発明に係る処理を遂行させることができる。

【００５０】以上の構成により、分離メモリ１８を備えたＩＣカード１では、分離メモリ１８へのアクセス権が設定されている仲介器２からのアクセス要求があった場合にのみ、上記したＣＰＵ２１等から構成されるデータ処理手段により分離メモリ１８へアクセスすることができる。すなわち、アクセス権を有する仲介器２からのアクセス要求があった場合にのみ、分離メモリ１８に格納されている秘匿性が高いデータを読み出すことや、書き換えることや、削除することや、液晶ディスプレイ１１に表示させることや、また、分離メモリ１８に新規なデータを記憶させること等を行うことができる。

【００５１】これにより、分離メモリ１８に記憶されている秘匿性が高いデータが、アクセス権を有しない第三者等によって読み出されてしまうことや、偽造或いは改変されてしまうことや、また、これら第三者による不正な行為に起因して不正なデータが取り引きされ、或いは流出してしまうこと等を防止することができ、当該データの安全性を更に高めることができる。また、本例のように、ＩＣカード１に備えられた表示手段（液晶ディスプレイ１１）によりＩＣチップ１７ａ～１７ｚに記憶されているデータを表示させることができる構成とした場合には、分離メモリ１８を備えて当該分離メモリ１８に

秘匿性が高いデータを格納し、これら秘匿性が高いデータの表示処理を上記したアクセス権により制御することにより、当該データの安全性を確保することもできる。

【００５２】また、ＩＣカード１の外部にある仲介器２からのアクセス要求がないと分離メモリ１８へアクセスすることができない構成のため、例えば１チップマイクロコンピュータ１６が不正に改造等された場合であっても、データの漏洩等を防止して当該データの安全性を確保することができる。また、誤った相手との取引処理等を防止するために、上記したようにＩＣカード１側で仲介器２のＩＤを認証するとともに、仲介器２側でもＩＣカード１のＩＤを認証し、これによりＩＣカード１と仲介器２との間で相互認証を行うことが好ましい。

【００５３】すなわち、例えば、アクセス権を有した仲介器２からのアクセス要求に応じて上記したＣＰＵ２１等から構成されるデータ処理手段が分離メモリ１８へアクセスする際に、分離メモリ１８に格納されている自己のＩＣカード１のＩＤを読み出して仲介器２へ通知するようにする。これにより、仲介器２では、通知されたＩＣカード１のＩＤが正しいものであるか否かを認証することができ、分離メモリ１８に格納されている秘匿性が高いデータが漏洩等してしまうことや、不正なＩＣカード１や不正な仲介器２との間でデータの通信が行われてしまうことを防止することができる。

【００５４】ここで、上記した分離メモリ１８におけるメモリの割当ての一例を図６を用いて説明する。なお、本例では、上記した残高データを例にして説明する。ここで、決済に関しての過去の取引内容である残高データの具体的なデータ内容としては、例えば取引日時や、支払い或いは受取を示す取引種別や、取引金額や、取引を行った仲介器２のＩＤや、取引を行った相手側のＩＣカードのＩＤや、取引前や取引後の残高或いは支払い可能金額といった資金データや、取引処理に際して仲介器２を介してシステム管理装置３から受信される後述する接続確認データや、これらを格納する後述するセル番号やエリア番号等といった取引の環境を示すデータが含まれる。

【００５５】図６（ａ）に分離メモリ１８の理論的なメモリの割当てを示すように、この分離メモリ１８には、理論的に分割した多数の格納エリアＲ１、Ｒ２、・・・が設けられており、また、各格納エリアＲ１、Ｒ２、・・・はそれぞれ２つのセルに分割されている。ここで、同図（ａ）では、例えばセルＡとセルＢ（格納エリアＲ１）、セルＣとセルＤ（格納エリアＲ２）、セルＥとセルＦ（格納エリアＲ３）、セルＧとセルＨ（格納エリアＲ４）、・・・といったように２つのセル毎に組となって点線で囲まれた各格納エリアＲ１、Ｒ２、・・・を構成している。

【００５６】また、図６（ａ）で上段にあるセルＡ，Ｃ，Ｅ，Ｇ、・・・には、上記した残高データが格納され、格納された残高データは新たな取引処理が行われた際に消去される。すなわち、残高データとしては、直前に行われた取引処理に関する残高データのみが保持されて、それ以前の取引処理に関する残高データについては消去されて消滅（無効化）させられる。また、下段にあるセルＢ，Ｄ，Ｆ，Ｈには、同一の格納エリア内のセルＡ，Ｃ，Ｅ，Ｇ，・・・に格納されていた残高データが消滅させられた際に、当該残高データがいかなる取引処理により消滅させられたかを示す消滅記録データが格納される。なお、これら残高データや消滅記録データには、例えば署名関数による署名といった取引処理の証拠が付される。

【００５７】図６（ａ）では、格納エリアＲ１のセルＡ及び格納エリアＲ２のセルＣに格納されていた残高データが消滅させられて黒く塗りつぶされており、これらの残高データについての消滅記録データがそれぞれセルＢ及びセルＤに格納されている。また、格納エリアＲ３のセルＥには、直前の取引処理に関する残高データが格納されており、この残高データは未だ消滅させられていないため、セルＦには未だ消滅記録データが格納されておらず、セルＦは未使用の空白状態である。ここで、例えば図６（ａ）の状態において、新たな取引処理が行われた場合には、分離メモリ１８の理論的なメモリ割当ての状態は図６（ｂ）に示すようになる。

【００５８】すなわち、新たな取引処理に関する残高データが格納エリアＲ４のセルＧに格納されるとともに、セルＥに格納されていた残高データが消滅させられ、このセルＥの残高データについての消滅記録データがセルＦに格納される。このようにして、新たな取引処理によって生成された最新の残高データのみが、取引の順序に従って加算されていく取引エリア番号（Ｒ１、Ｒ２、Ｒ３、Ｒ４、・・・）に対応した各格納エリアＲ１、Ｒ２、Ｒ３、Ｒ４、・・・に順次格納されていく。従って、上記のように最新の取引処理によって生成された残高データのみを分離メモリ１８に保持しておくようにすることにより、残高データの不正な複写や暗号解読等が行われてしまう可能性を低く抑えることができる。なお、分離メモリ１８のメモリ割当てとしては、必ずしも上記のような構成が用いられる必要はなく、例えばＩＣカード１により行われたすべての取引処理についての残高データを分離メモリ１８内に保持しておくようにする等、任意の構成が用いられてもよい。

【００５９】また、以上に示した各種類毎のデータについて設定されたパスワードデータによる複数種類のデータの一括管理処理や、ＩＣカード１に分離メモリ１８を備えて行われる分離メモリ１８へのアクセス制御処理については、それぞれの処理が別個に適用されてデータの安全性が担保されてもよく、また、本例のように、これらの処理が併用されてデータの安全性を更に担保するようにされてもよい。すなわち、例えばＩＣカード１に分

離メモリ１８を備えて当該分離メモリ１８へのアクセス制御処理のみを行う場合には、必ずしも本例のようにＩＣカード１に複数のＩＣチップ１７ａ～１７ｚが備えられていなくてもよく、例えばＩＣカード１に１個のＩＣチップ１７ａと１個の分離メモリ１８とを備えて、当該ＩＣチップ１７ａに記憶される１種類のデータについての秘匿性が高いデータを分離メモリ１８に記憶して、当該データの安全性を確保することもできる。

【００６０】また、例えば本例のように、ＩＣカード１に複数のＩＣチップ１７ａ～１７ｚと１個の分離メモリ１８とを備えることにより、これら複数のＩＣチップ１７ａ～１７ｚにより複数種類のデータをデータの種類毎に安全性を担保して一括管理するとともに、これら複数種類のデータについての秘匿性が高いデータを１個の分離メモリ１８にまとめて格納して当該分離メモリ１８へのアクセスを制御することにより、これら複数種類のデータについての秘匿性が高いデータを１個の分離メモリ１８で一括管理して、当該データの安全性を更に確実に担保することもできる。

【００６１】図７には、リーダ・ライタである仲介器２の一例を示してあり、この仲介器２には、アンテナＴ２と、無線データの通信を行う無線部６１と、当該通信の制御を行う制御部６２と、データの処理を行うコンピュータ６３と、外部からデータを入力するための操作キー６４と、外部にデータを表示するための液晶ディスプレイ６５と、データを記憶するメモリ６６と、時刻を計時する時計部６７と、これら各処理部６１～６７に電源を供給する電源６８とが備えられている。無線部６１は、無線通信を行うための例えば変調器や復調器を有しており、アンテナＴ２を介してＩＣカード１及びシステム管理装置３との間で無線データの通信を行う。

【００６２】制御部６２は、上記した無線部６１による無線データの通信処理を制御する手段を有しており、例えば無線部６１により受信されたデータをコンピュータ６３へ出力し、また、送信対象となるデータをコンピュータ６３から無線部６１へ出力する。コンピュータ６３は、ＣＰＵ７１やＰＲＯＭ７２やＲＡＭ７３を備えており、ＰＲＯＭ７２には、例えばＩＣカード１との間で行われる所定の取引プロトコルに基づく決済処理等といった仲介器２において行われる種々の処理を制御する制御プログラムが格納されている。そして、ＣＰＵ７１がＰＲＯＭ７２に格納されたこれらの制御プログラムをＲＡＭ７３に展開して実行することにより、決済等といった各種の取引処理や仲介器２全体を管理及び制御するための処理を行う。

【００６３】また、本例では、上記したＰＲＯＭ７２には、正規に登録されている各ＩＣカード１に設定されている上記した呼出番号や、各ＩＣカード１の分離メモリ１８へのアクセス権である自己の仲介器２のＩＤデータや、各ＩＣカード１のＩＣチップ１７ａ～１７ｚ毎に設定されているパスワードデータ等が格納されている。これにより、仲介器２がＩＣカード１へ無線データを送信する場合には、当該データの先頭等に宛先番号として、当該データの送信先となるＩＣカード１の呼出番号のデータが含められる。

【００６４】また、仲介器２がＩＣカード１の分離メモリ１８やＩＣチップ１７ａ～１７ｚへのアクセスを行う場合には、ＣＰＵ７１等により当該仲介器２に設定されているＩＤデータや、当該ＩＣチップ１７ａ～１７ｚに設定されているパスワードデータを読み出して、これらのデータを無線部６１及びアンテナＴ２を介してＩＣカード１へ送信する。なお、ＩＣカード１の分離メモリ１８へのアクセス権（ＩＤ）や各ＩＣチップ１７ａ～１７ｚへのアクセス権（パスワードデータ）の設定については、各仲介器２毎に行われてもよく、例えば或る仲介器２にはＩＣチップ１７ａ～１７ｃへのアクセス権のみを設定するということや、また、例えば或る仲介器２には分離メモリ１８へのアクセス権のみを設定するということもできる。

【００６５】操作キー６４は、例えばＩＣカード１の利用者によって操作されるキーであり、決済取引等において、利用者によって入力された取引金額や、取引を合意する取引合意認証等といったデータを受け付け、このようにして入力されたデータをコンピュータ６３へ出力する。液晶ディスプレイ６５は、データを表示するための手段であり、決済取引等において、取引が行われた金額や、利用者への各種メッセージ等を表示出力する。

【００６６】メモリ６６は、例えばコンピュータ６３によりデータを読み出すことのみが可能な記憶手段であり、このメモリ６６には、例えば決済処理を行うための所定プロトコルのデータや、仲介器２全体を管理するために必要な管理データや、このメモリ６６へのアクセス権を有したシステム管理装置３から受信された後述する接続確認データや、正規に登録されているＩＣカード１に設定されているＩＤデータや、不当なＩＣカード１のＩＤをリストアップしたブラックリストのデータ等といったデータが格納される。なお、このメモリ６６へのデータの書き込み処理は、例えばシステム供給者により管理されている当該メモリ６６へのアクセス権を有したリーダ・ライタによって行われる。また、例えば各仲介器２毎にメモリ６６へのアクセス権限を異ならせてもよい。

【００６７】以上の構成により、仲介器２は、ＩＣカード１との間でデータの通信を行うことによりＩＣカード１との間で決済処理等といった種々の処理を行い、また、例えば取引金額等といったデータを表すメッセージ信号をＩＣカード１へ送信することにより、こうしたメッセージを当該ＩＣカード１の液晶ディスプレイ１１に表示させる。また、仲介器２は、システム管理装置３との間でデータの通信を行うことにより、ＩＣカード１と

の間で行われた決済処理等といった各種処理の内容をシステム管理装置３に通知し、また、システム管理装置３から後述する接続確認データ等を受信する。

【００６８】図８には、システム管理装置３の一例を示してあり、このシステム管理装置３には、アンテナＴ３と、無線データの通信を行う無線部８１と、当該通信の制御を行う制御部８２と、データの管理等を行う管理センタ８３と、外部からデータを入力するための操作キー８４と、外部にデータを表示するための液晶ディスプレイ８５と、データを記憶するメモリ８６と、データを蓄積するデータベース８７と、これら各処理部８１～８７に電源を供給する電源８８とが備えられている。

【００６９】無線部８１は、無線通信を行うための例えば変調器や復調器を有しており、アンテナＴ３を介して仲介器２との間で無線データの通信を行う。制御部８２は、上記した無線部８１による無線データの通信処理を制御する手段を有しており、例えば無線部８１により受信されたデータを管理センタ８３へ出力し、また、送信対象となるデータを管理センタ８３から無線部８１へ出力する。管理センタ８３は、例えばプロセッサやメモリ等から構成されており、図１に示した本例のＩＣカードシステム全体の運営管理処理を行い、本システムに含まれるすべてのＩＣカード１及びすべての仲介器２のＩＤ等といったデータや、これらＩＣカード１と仲介器２との間で行われた決済処理等といったすべての処理に関するデータを後述するデータベース８７により管理する。

【００７０】なお、上記したように、ＩＣカード１と仲介器２との間で行われた取引処理等のデータは、例えば当該取引処理が終了した後に、仲介器２からシステム管理装置３に通知される。また、管理センタ８３には、時刻を計時する手段が備えられており、管理センタ８３は、この手段により計時された時刻のデータ等を含む接続確認データを例えば一定時間毎に更新して作成し、これをデータベース８７に格納しておく。また、このようにして随時作成された接続確認データを仲介器２へ適時通知することにより、管理センタ８３と後述するデータベース８７や仲介器２との間の接続状況を確認する処理を行う。

【００７１】すなわち、上記したように、管理センタ８３により発行された接続確認データは、仲介器２や当該仲介器２との間で取引処理を行ったＩＣカード１に通知され、この結果、システム管理装置３と仲介器２とＩＣカード１とに共通の接続確認データが格納される。このため、ＩＣカード１や仲介器２がシステム管理装置３と同一の接続確認データを格納しているか否かを検査することにより、正規の接続確認データを有していない不正な取引処理等を検出することができる。選択キー８４は、システム管理装置３を供給するシステム供給者等により操作されるキーであり、例えばシステム供給者はこのキー８４を操作することにより、データベース８７に蓄積されているデータを検索等することができる。また、液晶ディスプレイ８５は、データを表示するための手段であり、上記のようにしてシステム供給者により検索されたデータ等を表示出力する。

【００７２】メモリ８６は、例えば管理センタ８３からはデータの読み出しのみが可能な記憶手段であり、このメモリ８６には、例えば仲介器２との間で行われるデータ通信のプロトコルのデータが格納されている。なお、このメモリ８６へのデータの書き込み処理についても、上記した仲介器２の場合と同様に、例えばシステム供給者によって管理されている当該メモリ８６へのアクセス権を有したリーダ・ライタによって行われる。

【００７３】データベース８７は、上記したように、すべてのＩＣカード１とすべての仲介器２との間で行われた取引処理等に関するデータや、上記した接続確認データ等を蓄積する。また、このデータベース８７には、不当なＩＣカード１や仲介器２のＩＤをリストアップしたブラックリストのデータが格納されている。また、上記図１に示したように、システム管理装置３の管理センタ８３には、ＡＴＭ交換機５が接続されており、このＡＴＭ交換機５を介して通信販売会社６のＬＡＮ７や官公庁機関８のコンピュータ９等との間でデータの通信を行うこともできる。

【００７４】以上の構成により、システム管理装置３は、この管理装置３が管理するＩＣカードシステムに備えられたすべてのＩＣカード１及びすべての仲介器２のデータや、これらＩＣカード１と仲介器２との間で行われるすべての取引処理等に関するデータを格納して管理する。また、システム管理装置３では、上記したＡＴＭ交換機５を介して各会社や官公庁機関等に備えられているコンピュータ等との間でデータの通信を行うことにより、例えばＩＣカード１により行われた決済処理のデータを通信販売会社６に通知することや、また、例えばＩＣカード１により行われた免許証の住所変更等のデータを官公庁機関に通知することを行う。

【００７５】次に、上記したＩＣカード１及びＩＣカードシステムにより行われる処理の手順を図面を参照して説明する。なお、本例では、ＩＣカード１には、上記図３に示したように、複数のＩＣチップ１７ａ～１７ｚと分離メモリ１８とが備えられているとし、分離メモリ１８にはＩＣチップ１７ａ～１７ｚに比べて秘匿性が高いデータが記憶されているとする。図９には、ＩＣカード１のＩＣチップ１７ａ～１７ｚに記憶されているデータを各ＩＣチップ毎（データの種類毎）に設定されているパスワードデータを用いて表示させる処理の手順を示してある。なお、この処理は、利用者がＩＣカード１を操作することによって行われる。

【００７６】まず、選択キー１２によりＩＣカード１の電源がＯＮにされ（ステップＳ１）、選択キー１２やスクロールキー１３によりこのＩＣカード１に設定されて

いるカード暗証番号が入力される（ステップＳ２）。ここで、カード暗証番号とは、ＩＣカード１を利用するために設定されている暗証番号のことであり、この暗証番号を正しく入力することによりＩＣカード１の種々の機能を利用することができるようになる。すなわち、ＩＣカード１に入力されたカード暗証番号が誤っていた場合にはＩＣカード１を利用することができず、また、ＩＣカード１により入力誤りの回数をカウントすることにより、例えばｎ（ｎは１以上の整数）回連続して誤ったカード暗証番号が入力された場合には、安全性の確保のために、後述する図１２のカード暗証番号の初期設定処理をシステム供給者により行ってもらわなければ、ＩＣカード１を使用することができなくなるような設定になっている（ステップＳ７）。

【００７７】また、カード暗証番号が正しく入力されるとＩＣカード１の各種機能が利用可能な状態になり、次に、ＩＣカード１のキー１２、１３により表示を行うモードが設定され、また、同様にして利用者により液晶ディスプレイ１１に表示させたいＩＣチップ番号が指定される（ステップＳ３）。ここで、ＩＣチップ番号の入力としては、例えば各ＩＣチップ１７ａ～１７ｚ毎に設定された番号を入力するという構成であってもよく、また、例えば各ＩＣチップ１７ａ～１７ｚに記憶されているデータの種類（名称）を指定することにより当該ＩＣチップを特定するという構成であってもよい。

【００７８】次に、上記のようにして指定されたＩＣチップ（ＩＣチップ１７ａ～１７ｚのいずれか）に設定されているパスワードデータ（確認事項）が入力される（ステップＳ４）。なお、このパスワードデータについても、上記したカード暗証番号と同様に、正しく入力されなかった場合にはデータの表示が行われず、また、この入力誤りの回数をカウントすることにより、例えばｍ（ｍは１以上の整数）回連続して誤ったパスワードデータが入力されると、システム供給者に依頼しなければＩＣカード１が使用不可能な状態となる（ステップＳ８）。また、正しいパスワードデータが入力されると、指定されているＩＣチップに記憶されている例えば記録データといったデータや、当該ＩＣチップのチップ番号やデータの種類等が液晶ディスプレイ１１に表示出力され（ステップＳ５）、これにより、利用者は各ＩＣチップ１７ａ～１７ｚに記憶されているデータの内容を見ることができる（ステップＳ６）。

【００７９】以上のように、各ＩＣチップ１７ａ～１７ｚ毎に設定されているパスワードデータを正しく入力しないと、これら各ＩＣチップ１７ａ～１７ｚに記憶されているデータを表示させることができないため、これらのデータの漏洩等を防止して当該データの安全性を担保することができる。また、上記したＩＣカード暗証番号や各ＩＣチップ１７ａ～１７ｚ毎に設定されているパスワードデータは利用者により変更が可能であり、この変更処理の手順を図１０に示す。なお、この処理についても、利用者がＩＣカード１を操作することによって行われる。

【００８０】まず、上記と同様に、ＩＣカード１の電源がＯＮにされ（ステップＳ１１）、カード暗証番号が入力されてカードロックが解除される（ステップＳ１２）。なお、誤ったカード暗証番号が入力された場合については上記と同様である（ステップＳ２２）。次に、このカード暗証番号を変更する場合には当該変更を行うモードが設定され（ステップＳ１３）、例えば古いカード暗証番号（旧番号）や新たに設定されるカード暗証番号（新番号）が利用者により入力されて確認が行われ（ステップＳ１４）、これによりカード暗証番号の変更処理が行われる。

【００８１】また、各ＩＣチップ毎に設定されているパスワードデータの変更（ロック厳重機能設定）処理を行う場合には当該変更を行うモードが設定され（ステップＳ１５）、まず、パスワードデータの変更を行う対象となるＩＣチップ番号が指定されて（ステップＳ１６）、指定されたＩＣチップに設定されているパスワードデータ（確認事項）が入力される（ステップＳ１７）。なお、誤ったパスワードデータが入力された場合については上記と同様である（ステップＳ２３）。また、正しいパスワードデータが入力された場合には、パスワードデータの変更処理が可能となり、利用者によってパスワードデータの再設定処理が行われて（ステップＳ１８）、パスワードデータの書き換えが行われる（ステップＳ１９）。なお、他のＩＣチップに設定されているパスワードデータの変更についても上記と同様である。

【００８２】また、パスワードデータの設定としては、例えば１つのＩＣチップ１７ａ～１７ｚに複数の確認事項をパスワードデータとして設定することもでき、この場合には、例えば利用者に好みや必要性に応じて、各ＩＣチップ１７ａ～１７ｚ毎にパスワードデータとして設定される氏名や生年月日等といった確認事項の数を増加させることや、減少させることもできる。また、例えば使用頻度が少ないＩＣチップ１７ｑに多くの確認事項をパスワードデータとして設定して、更なるロックをかけておくといったこともできる。

【００８３】このように各ＩＣチップ毎に異なった数の確認事項を設定することにより、各ＩＣチップ毎に記憶されるデータの種類等に応じて、これら各種類毎のデータの安全性を確保することができる。また、上記のようにしてカード暗証番号やパスワードデータの変更処理が終了し、例えば選択キー１２によりＩＣカード１の電源がオフに設定されると、ＩＣカード１がロック（カードロック）され（ステップＳ２０）、再び電源をＯＮにしてカード暗証番号を入力しないとＩＣカード１が利用できない状態になる（ステップＳ２１）。

【００８４】なお、ＩＣカード１の利用者により用いら

れるパスワードデータと仲介器２により用いられるパスワードデータとが共通である場合には、上記のようにして変更されたパスワードデータが、例えば次回の取引処理の際にＩＣカード１から仲介器２に通知される。また、例えば、上記のパスワードデータ変更処理が、ＩＣカード１と仲介器２との間でデータの通信を行うことができる状態でのみ行われるといった構成としてもよく、この場合には、上記した変更処理の際に、変更後のパスワードデータがＩＣカード１から仲介器２に通知される。

【００８５】次に、図１１には、ＩＣカード１と仲介器２との間で行われる決済取引等の処理の手順を示してある。まず、利用者によりＩＣカード１が仲介器２の設置されている場所へ持って行かれ（ステップＳ３１）、当該ＩＣカード１の電源がＯＮにされて、当該ＩＣカード１が仲介器２との間でデータの通信を行うことができる距離に近接させられる（ステップＳ３２）。このようにしてＩＣカードがセットされると、次に、上記と同様に、ＩＣカード１にカード暗証番号が入力されてカードロックが解除される（ステップＳ３３）。なお、誤ったカード暗証番号が入力された場合については、上記と同様である（ステップＳ４２）。

【００８６】次に、取引処理を行うＩＣチップ番号がＩＣカード１に入力され（ステップＳ３４）、このようにして指定されたＩＣチップに設定されているパスワードデータ（確認事項）が入力される（ステップＳ３５）。なお、誤ったパスワードデータが入力された場合については、上記と同様である（ステップＳ４３）。また、正しいパスワードデータが入力されると、指定されたＩＣチップに記憶されている例えばクレジットのデータや（ステップＳ３６）、各種身分証明のデータや（ステップＳ３７）、小口決済の残金のデータ（ステップＳ３８）等といったデータがＩＣカード１の液晶ディスプレイ１１に表示され、利用者がＩＣカード１を操作することにより当該ＩＣカード１と仲介器２との間で各種取引が行われる。

【００８７】具体的には、例えば小口決済において、利用者ＡがＩＣカード１Ａから他の利用者ＢのＩＣカード１Ｂへ１万円を振り込む場合には、まず、利用者ＡがＩＣカード１Ａを操作して利用者ＢのＩＣカード１Ｂへ１万円を振り込むための手続きを行う。これにより、利用者ＡのＩＣカード１Ａと仲介器２との間でデータの通信が行われ、利用者ＡのＩＣカード１Ａに記憶されている当該小口決済についての残高（例えば上記した記録データ）から１万円が減少させられる。また、利用者ＢのＩＣカード１Ｂについては、例えば利用者Ｂが上記仲介器２或いは他の場所に設置されている仲介器により次回の取引を行う際に、当該ＩＣカード１Ｂに記憶されている上記小口決済についての残高（例えば上記した記録データ）に１万円が増加させられる。このようにして、利用者ＡのＩＣカード１Ａから利用者ＢのＩＣカード１Ｂへ金銭の振り込み処理が行われる。

【００８８】なお、上記したように、ＩＣカード１と当該ＩＣカード１の分離メモリ１８へのアクセス権が設定されている仲介器２との間で取引処理が行われた場合には、上記した記録データの更新処理と共に、分離メモリ１８に記憶されている例えば上記した残高データといったデータの更新処理が行われる場合もある。また、上記したように、例えば利用者ＡのＩＣカード１Ａに格納される記録データや残高データには、利用者ＢのＩＣカード１Ｂや仲介器２による署名が行われ、同様に、利用者ＢのＩＣカード１Ｂに格納される記録データや残高データには、利用者ＡのＩＣカード１ＡやＩＣカード１Ｂとの間で取引処理を行った仲介器による署名が行われる。

【００８９】また、ＩＣカード１と仲介器２との間でデータの通信を行うことにより、例えば免許証の住所といった各種身分証明データの変更処理を行うこともできる。すなわち、例えば分離メモリ１８に記憶されている免許証の住所を変更させる手続きがＩＣカード１に対して利用者により行われた場合には、アクセス権を有した仲介器２が当該分離メモリ１８に記憶されている免許証の住所のデータを変更させるとともに、当該変更後の住所データをシステム管理装置３へ送信する。また、システム管理装置３では、仲介器２から受信した住所変更のデータをＡＴＭ交換機５を介して官公庁機関８のコンピュータ９へ送信し、これにより、官公庁機関８では、受信したデータに基づいて、コンピュータ９等に登録されている上記した利用者の免許証の住所データの内容を変更させる。

【００９０】なお、ＩＣカード１と仲介器２との間で行われる取引等の処理としては、上記したものに限られず、利用者の要求等に応じて種々の取引処理が行われてもよい。また、取引処理が終了した後には（ステップＳ３９）、例えばＩＣカード１を再びカード暗証番号やパスワードデータを入力しなければ利用することができない状態にカードロックして（ステップＳ４０）、仲介器１との間のデータの通信を終了させる（ステップＳ４１）。以上のようにして、ＩＣカード１では、決済取引等といった種々の処理を例えば他のＩＣカードとの間で仲介器２を介して行うことができる。また、ＩＣカード１の分離メモリ１８へのアクセス権を有した仲介器２との間でデータの通信が行われる場合にのみ、当該仲介器２からの要求に応じて例えば残高データといった分離メモリ１８内の秘匿性が高いデータが更新等されるため、分離メモリ１８に記憶されているデータの安全性を確実に担保することができる。

【００９１】また、以上では、ＩＣカード１と仲介器２との間で取引処理等を行うに際して、ＩＣカード１の選択キー１２やスクロールキー１３によりカード暗証番号やパスワードデータの入力処理を行い、ＩＣカード１の

液晶ディスプレイ１１により各種データの表示処理を行ったが、これら入力処理や表示処理は、例えば仲介器２に備えられている操作キー６４や液晶ディスプレイ６５により行われてもよい。また、これらの入力処理や表示処理をＩＣカード１と仲介器２との両方の装置で行うようにすることにより、パスワードデータ等の検査をこれら両装置で二重に行って確認するようにすることもできる。

【００９２】次に、ＩＣカード１の初期設定及びロック解除処理の手順を図１２を用いて説明する。なお、これらの処理は、例えばシステム供給者や各会社及び機関等が有している初期設定用のリーダ・ライタにより行われ、本例では、このリーダ・ライタとＩＣカード１とを直接的に接点で接続して以下に示す初期設定及びロック解除処理を行う。また、このリーダ・ライタは、ＩＣカード１の分離メモリ１８へのアクセス権を有している。ここで、初期設定処理とは、未だ発行されていないＩＣカード１に上記したＩＤやカード暗証番号等を設定する処理のことである。また、ロック解除処理とは、利用者がＩＣカード１のパスワードデータ等を忘れてしまった場合や、上記図９、１０、１１で示したように、誤ったパスワードデータの入力によりＩＣカード１が利用者自身では使用不可能な状態となってしまった場合に、このＩＣカード１のカードロックの状態を解除する処理のことである。

【００９３】すなわち、初期設定或いはロック解除処理に際しては（ステップＳ５１）、まず、例えば上記のように初期設定用リーダ・ライタとＩＣカード１とが接点で接続される（ステップＳ５２）。ここで、初期設定処理が行われる場合には（ステップＳ５３）、例えば各ＩＣカード１の通し番号や、各ＩＣカード１に固有な上記したＩＤといったデータがＩＣカード１の分離メモリ１８に書き込まれ（ステップＳ５４）、カード暗証番号の初期設定が行われる（ステップＳ５５）。これにより、例えば新規な利用者に対して、初期化された新規なＩＣカード１が発行される（ステップＳ５６）。なお、利用者は、上記図１０に示したように、初期に設定されたカード暗証番号を任意に変更させることができる。

【００９４】また、ロック解除処理が行われる場合には（ステップＳ５３）、リーダ・ライタによりＩＣカード１の分離メモリ１８に書き込まれている通し番号やＩＤ等が読み込まれ（ステップＳ５７）、読み込まれた通し番号等が当該ロック解除処理を申請した者に対して正規に登録されたものであるか否かが判定される（ステップＳ５８）。なお、この判定としては、例えば申請者の身分証明や住所等のデータ（個人データ）とＩＣカード１に格納されている個人データとが一致するか否かを判定することにより行うこともできる。ここで、ＩＣカード１が当該申請者に対して正規に登録されたものであると判定された場合には、ＩＣカード１のロックが解除されて、新たなカード暗証番号やパスワードデータが設定される（ステップＳ５５）。このようにして、ロック解除処理が行われたＩＣカード１は、再び通常通りに利用者によって利用可能な状態となる（ステップＳ５６）。

【００９５】また、ＩＣカード１が例えば申請者が不正に入手したものであったために、当該ＩＣカード１が当該申請者に対して発行されたものではないことが判定された場合には、例えばｐ（ｐは１以上の整数）回の再確認処理や再試行処理が行われる。そして、これらの処理によっても当該申請者の個人データとＩＣカード１に記憶されている個人データとが一致しないことが確認された場合には、例えば当該ＩＣカード１が没収される（ステップＳ５９）。以上のようにして、ＩＣカード１の初期設定及びロック解除処理を行うことができ、また、正規に登録されていない第三者によりＩＣカード１が不正に利用されてしまうことを防止することができる。

【００９６】次に、ＩＣカード１の各ＩＣチップ１７ａ～１７ｚへデータを書き込む処理を図１３を用いて説明する。なお、この処理も、例えばシステム供給者や各会社及び機関等が有しているデータ書き込み用のリーダ・ライタにより行われ、また、ＩＣカード１には各ＩＣチップ毎のパスワードデータが未だ設定されていない状態であるとする。また、上記したように、以下の書き込み処理においては、複数種類のデータがデータの種類毎に各ＩＣチップ１７ａ～１７ｚに書き込まれる。データ書き込み処理に際しては、まず、例えばリーダ・ライタとＩＣカードとが接点で接続され（ステップＳ６１）、ＩＣカード１にカード暗証番号が入力されてカードロックが解除される（ステップＳ６２）。なお、誤ったカード暗証番号が入力された場合については、上記と同様である（ステップＳ６８）。

【００９７】次に、データを書き込む対象となるＩＣチップ番号が入力され（ステップＳ６３）、この指定された例えばＩＣチップ１７ｚに既にデータが書き込まれているか否かを確認する（ステップＳ６４）。ここで、指定されたＩＣチップ１７ｚにデータが書き込まれていなければ、当該ＩＣチップ１７ｚに上記した記録データ等といった必要なデータが新たに書き込まれ（ステップＳ６５）、当該ＩＣチップ１７ｚや他のＩＣチップ１７ａ～１７ｙについてのパスワードデータが各ＩＣチップ１７ａ～１７ｚ毎に登録されて（ステップＳ６６）、データ書き込み処理が終了される（ステップＳ６７）。また、指定されたＩＣチップ１７ｚに既にデータが書き込まれていた場合には、例えば書き込まれているデータが消去されてもよいか否かが各会社や機関等に再確認され、よければ当該データが消去されて（ステップＳ６９）、新たなデータが書き込まれ（Ｓ６３～Ｓ６５）、また、パスワードデータが設定される（ステップＳ６６～Ｓ６７）

【００９８】このようにして、複数種類のデータがデー

タの種類毎にＩＣカード1のＩＣチップ17ａ～17ｚに書き込まれ、また、各ＩＣチップ17ａ～17ｚ毎にパスワードデータが設定されて利用者により利用可能な状態となる。すなわち、上記図12で示した初期設定処理により発行されたＩＣカード1に、上記図13で示したパスワードデータの設定処理等を施すことにより、当該ＩＣカード1を利用者により利用可能な状態とすることができる。また、各ＩＣチップ17ａ～17ｚ毎にパスワードデータを設定するため、各種類毎のデータの安全性を担保しつつ、複数種類のデータを一括管理することができる。なお、上記図12で示した初期設定用のリーダ・ライタの機能や上記図13で示したデータ書き込み用のリーダ・ライタの機能は、仲介器2やシステム管理装置3に備えることもでき、この場合には、これら仲介器2やシステム管理装置3により上記図12や図13で示した処理をＩＣカード1に対して施すことができる。

【0099】以上説明したように、ＩＣカード1では、複数種類のデータを一括管理することができ、且つ、これら複数種類のデータをデータの種類毎に安全性を担保することができる。また、ＩＣカード1に分離メモリ18を設けて当該分離メモリ18へのアクセスを制御することにより、当該分離メモリ18に記憶される秘匿性が高いデータの安全性を更に高めることができる。また、上記したように、複数種類のデータをデータの種類毎に安全性を担保して一括管理しつつ、これら複数種類のデータについて秘匿性が高いデータを分離メモリ18に格納しておくこともでき、この場合には、例えば複数種類のデータについて秘匿性が高いデータを1個の分離メモリ18で一括管理して、且つ、当該データの安全性を確実に担保して保持しておくことができる。

【0100】また、本例のように、種々のデータを電子化して1枚のＩＣカードで管理することにより、利用者は、この1枚のＩＣカードを携帯することにより、これら種々の取引処理等を行うことができる。また、こうしたＩＣカードは軽量で安全な形状となっているため、持ち運びに便利であり、また、ＩＣカードに利用者自身の身分証明のデータを格納しておくことにより、例えば事故が生じた等といった非常時に当該利用者の身元の確認をとることを容易にすることもできる。すなわち、こうした緊急時にのみ警察等でＩＣカードのロックを解除することができるように法律的な基盤を確立しておくことにより、警察等では、必要に応じてＩＣカードに記憶されている身分証明のデータから当該ＩＣカードの利用者の身元を確認することができる。

【0101】また、同様に、例えば医療機関等の患者により、当該患者の健康保険証のデータや、医療機関等により作成されるカルテ等のデータを記憶させたＩＣカードが携帯されるようにし、また、当該データを医療機関等の間で任意に確認することができるように共有することにより、各医療機関等では、当該患者の健康状態のデータ等を即座に確認して対応することができる。また、上記実施例で示したように、運転免許証等といった身分証明のデータをＩＣカードに記憶させ、また、官公庁機関のネットワーク化等の基盤を整備することにより、例えばＢ－ＩＳＤＮのサービス対応により免許証の住所変更等の手続きをオンラインで行うようにすることもできる。

【0102】また、同様に、上記実施例で示したように、決済等の取引処理を例えば無線通信やネットワークを介して行うこともでき、また、利用者は、各個人毎に必要な種類のデータを自己のＩＣカードに記憶させておくことにより、複数種類のデータについての取引処理を1枚のＩＣカードで行うことができる。また、上記したＩＣカードの利用分野の一例として、例えば、或るＩＣカードに記憶されている残高額から他のＩＣカードに記憶されている残高額へ金額の移動を安全に行うことができるシステムが実現されれば、利用者は、小型のＩＣカードに小口決済の一部だけを電子マネーとして格納して持ち歩くこともできる。また、このようにＩＣカードを電子財布として用いることにより、現金が有する匿名性や流通性（譲渡性）等といった利点を損なうことなく、高い安全性を有する電子小口決済システムを実現することができる。

【0103】また、ＩＣカードは、例えば紙やプラスティック等から構成されるカードにデータを記憶等するＩＣチップを埋め込むことにより作成される。ここで、本発明では、複数種類のデータを管理するに際して複数枚のＩＣカードを備える必要はなく、これら複数種類のデータを1枚のＩＣカードで一括管理するようにしているため、紙やプラスティック等といった資源の使用量を少なく抑えることができ、これにより、資源の使用削減を実現することができる。

【0104】また、例えば利用者の要求や必要性に応じて、種々の形状を有するＩＣカードを作成することもでき、また、例えばＩＣカードを防水加工することにより、プール等といった水の中においてもＩＣカードを使用可能な状態にすることもできる。また、上記実施例のように、複数種類の会社や機関等の仲介器を1つのシステム管理装置によって管理するようにすることにより、ＩＣカードの利用者は、例えばＡ社の預金の残高を用いて直接的にＢ社の決済処理を行うといったように、異なる種類のデータ間（例えば異なる種類の会社間）での取引処理を行うこともできる。

【0105】

【発明の効果】以上説明したように、本発明に係るＩＣカードによると、例えば複数のメモリを備えることにより、複数種類のデータをデータの種類毎に記憶して、各種類のデータを記憶するメモリ毎に当該メモリへアクセスするためのパスワードデータを設定するようにしたた

め、１枚のＩＣカードで複数種類のデータを一括管理することができるとともに、これらのデータの安全性（セキュリティ）をデータの種類毎に担保することができる。また、本発明に係るＩＣカードによると、例えばデータを記憶するメモリと、当該メモリに記憶されるデータに比べて秘匿性が高いデータを記憶する分離メモリとを備え、分離メモリへのアクセス権が設定された外部のリーダ・ライタからのアクセス要求があった場合にのみ、当該分離メモリへのアクセスが可能となるようにしたため、当該分離メモリに記憶される秘匿性が高いデータの安全性を担保することができる。

【図面の簡単な説明】

【図１】本発明の一実施例に係るＩＣカードを用いたＩＣカードシステムの一例である。

【図２】本発明に係るＩＣカードの外観の一例である。

【図３】本発明に係るＩＣカードの一構成例である。

【図４】ＩＣカードに備えられるアンテナの構成例である。

【図５】ＩＣカードの二次電池の充電処理を説明するための図である。

【図６】ＩＣカードの分離メモリのメモリ割当ての一例を説明するための図である。

【図７】仲介器の一構成例である。

【図８】システム管理装置の一構成例である。

【図９】ＩＣカードによるデータ表示処理の手順の一例である。

【図１０】ＩＣカードによるパスワード等の変更処理の手順の一例である。

【図１１】ＩＣカードと仲介器との間で行われる決済取引等の処理の手順の一例である。

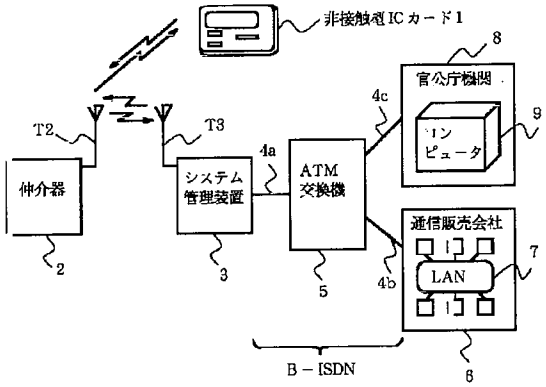
【図１２】ＩＣカードの初期設定及びロック解除処理の手順の一例である。

【図１３】ＩＣカードのＩＣチップへのデータ書き込み処理の手順の一例である。

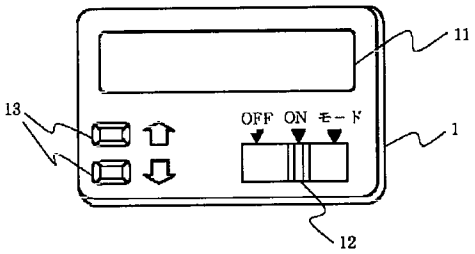
【符号の説明】

１・・ＩＣカード、　２・・仲介器、　３・・システム管理装置、４ａ、４ｂ、４ｃ・・回線、　５・・ＡＴＭ交換機、６・・通信販売会社、　７・・ＬＡＮ、　８・・官公庁機関、９・・コンピュータ、　Ｔ２、Ｔ３・・アンテナ１１・・液晶ディスプレイ、　１２・・選択キー、　１３・・スクロールキー、Ｔ１・・アンテナ、・１４・・無線部、１５・・制御部、１６・・１チップマイクロコンピュータ、　１７ａ～１７ｚ・・ＩＣチップ、１８・・分離メモリ、　１９・・二次電池、　２１・・ＣＰＵ、２２・・ＰＲＯＭ、　２３・・ＲＡＭ、５５・・コイル、　５６・・整流器、

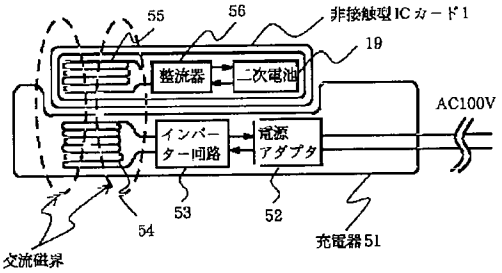
【図１】



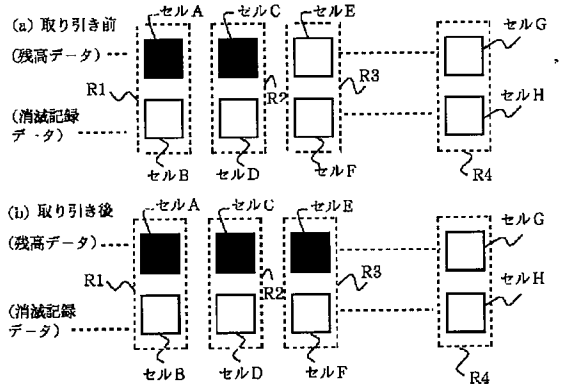
【図２】



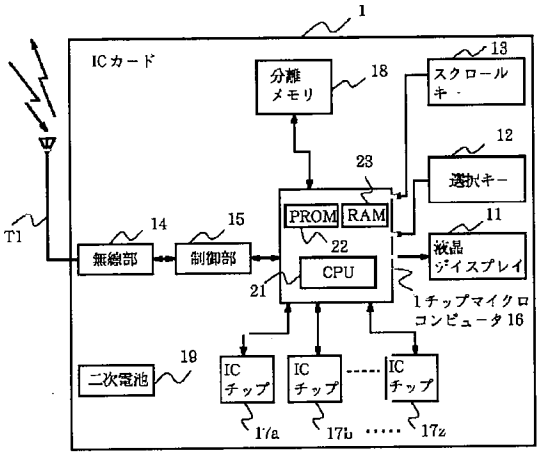
【図５】



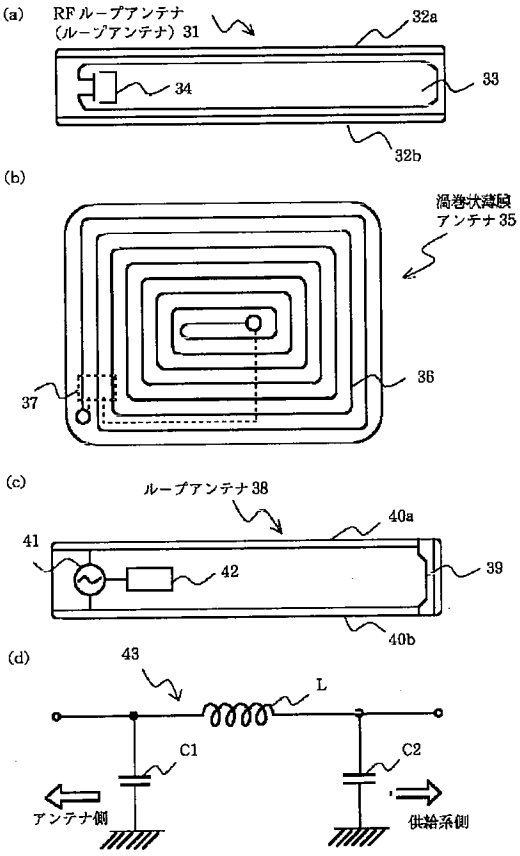
【図６】



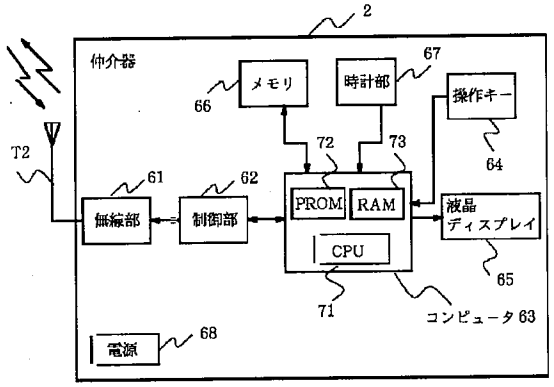
【図3】


1
ICカード
分離メモリ
18
スクロールキー
13
選択キー
12
23
PROM
RAM
22
液晶ディスプレイ
11
T1
14
無線部
15
制御部
CPU
21
1チップマイクロコンピュータ16
二次電池
19
IC チップ
IC チップ
IC チップ
17a
17b
17z

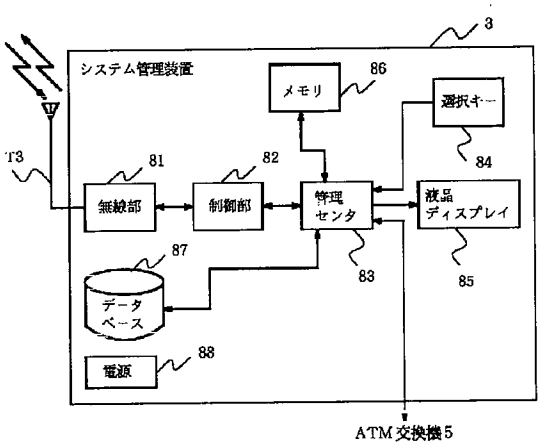
【図4】


(a)
RFループアンテナ（ループアンテナ）31
32a
34
33
32b
(b)
渦巻状薄膜アンテナ35
37
36
(c)
ループアンテナ38
40a
41
42
39
40b
(d)
43
L
C1
C2
アンテナ側
供給系側

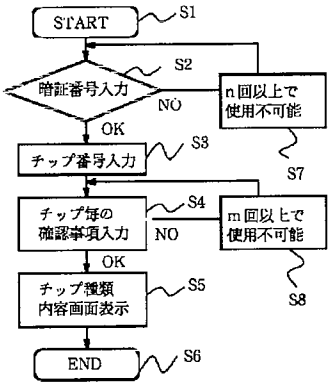
【図7】


2
仲介器
メモリ
66
時計部
67
操作キー
64
T2
72
73
61
62
無線部
制御部
PROM
RAM
液晶ディスプレイ
CPU
65
71
コンピュータ63
電源
68

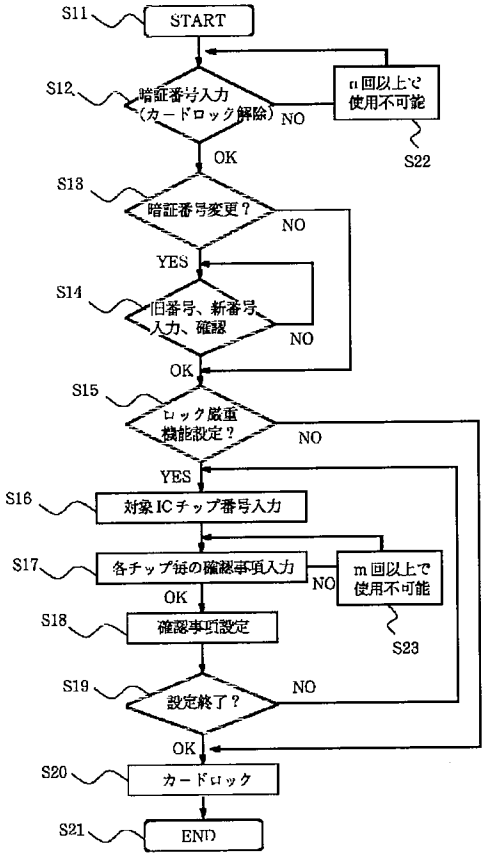
【図8】


3
システム管理装置
メモリ
86
選択キー
84
T3
81
82
無線部
制御部
管理センタ
液晶ディスプレイ
87
83
85
データベース
電源
88
ATM交換機5

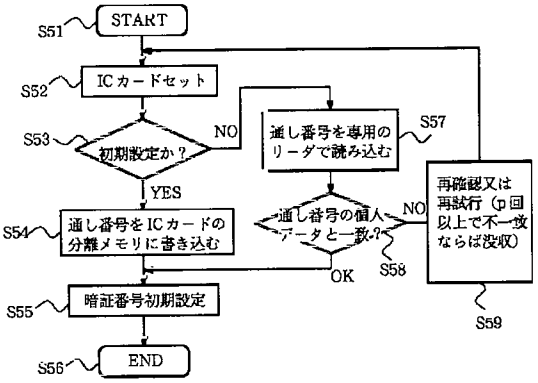
【図9】



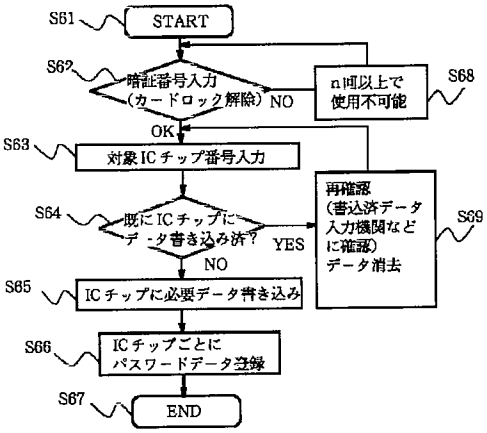
【図10】



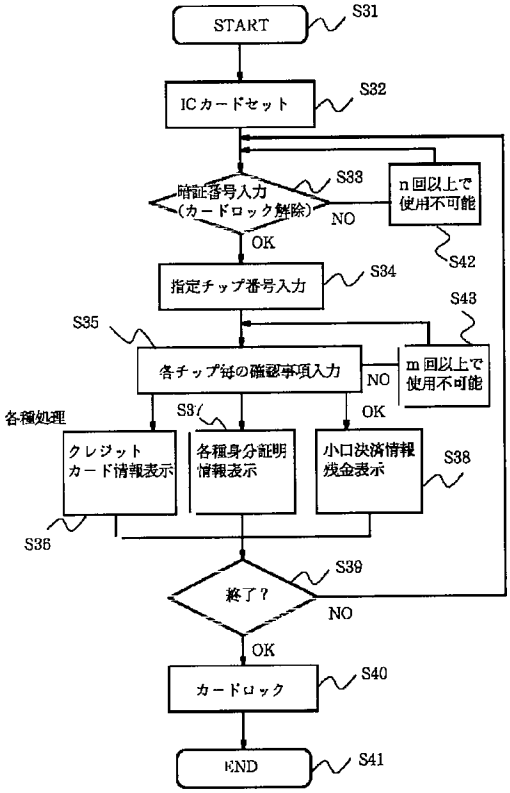
【図12】



【図13】



【図11】


START
S31
ICカードセット
S32
暗証番号入力
(カードロック解除)
S33
NO
n回以上で
使用不可能
S42
OK
指定チップ番号入力
S34
S43
S35
各チップ毎の確認事項入力
NO
m回以上で
使用不可能
各種処理
S37
OK
クレジット
カード情報表示
各種身分証明
情報表示
小口決済情報
残金表示
S38
S36
終了？
S39
NO
OK
カードロック
S40
END
S41